

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2019 AUG 20 PM 2:39

3:19 mj 512

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

814 Princeton Avenue, Fairborn, OH 45324, and the
electronic search of an Iphone, assigned cell #
937-424-7713, in possession of Susan Grooms

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1028	Identify Theft
18 U.S.C. 1343	Wire Fraud
18 U.S.C. 1956 and 1967	Money Laundering

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 08/20/2019

City and state: Dayton, Ohio

Terry Hedrick

Applicant's signature

TERRY HEDRICK, SA w/USSS

Printed name and title

Michael J. Newman

Judge's signature

MICHAEL J. NEWMAN, U.S. MAGISTRATE JUDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR
SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:
814 Princeton Avenue, Fairborn, OH 45324,
and the seizure and electronic search of an
Iphone, assigned cell # 937-424-7713, in the
possession of Susan Grooms

Case No. _____

3:19mj512MM

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Terry Hedrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of the above-captioned property, —which includes an electronic device — and the extraction from that property of electronically stored information from the electronic device, which is described in Attachment B.

2. I am a duly sworn Special Agent of the United States Secret Service (USSS), have been so employed such since October 2004. I have been in law enforcement since January 1989. My current investigative duties focus primarily on conducting criminal investigations involving counterfeiting of United States currency, forgery, bank fraud, false loan applications, wire fraud, credit card fraud, false identification, other financial crime investigations, and protective intelligence/threat investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The warrant is requested to search the residence located at 814 Princeton Avenue, Fairborn, OH 45324 for the iPhone smart phone device, which is assigned number 937-424-7713 (hereinafter, the “subject device.”) The subject device is believed to contain evidence that relates to violations of 18 U.S.C. § 1028 (identity theft), 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. §§ 1956 and 1957 (money laundering) have been committed. The warrant also seeks to search the subject device as detailed in paragraph 6.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents/officers and witnesses.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is 814 Princeton Avenue, Fairborn, OH 45324 (hereinafter, “814 Princeton Avenue”). Agents are requesting to search 814 Princeton Avenue for the subject device, which is believed to be in the possession of Susan Grooms (hereinafter, “GROOMS”), who resides at 814 Princeton Avenue, Fairborn, OH 45324. Thus, there is probable cause to believe the subject device will be located at 814 Princeton Avenue.

6. The applied-for warrant would authorize the search of 814 Princeton Avenue to locate and seize the subject device as well as conduct a forensic examination of the subject device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

Background

7. From on or about May 2018 to July 2019, PATRCIA DUDDING has been involved in an international wire fraud, mail fraud and money laundering schemes with SUSAN GROOMS, COLLEN BISHOP, and an individual believed to be from Nigeria who is known as LUCAS, in orchestrating numerous individual scams across the United States, Poland, Sweden and Australia. The investigation uncovered numerous victims who funneled their money to DUDDING, CAMPBELL, BISHOP and GROOMS' bank accounts, at the direction of LUCAS.

8. The victims in this investigation sent these funds to DUDDING, BISHOP and GROOMS' bank accounts via wire transfers, Cashier Checks, personal checks, Western Union, and Money Gram. DUDDING, BISHOP and GROOMS also transferred large sums of money between themselves during the scheme.

9. DUDDING voluntarily agreed to be interviewed by investigators several times beginning in June of 2019.

10. DUDDING informed law enforcement that she had over 23 years working in the banking industry working in new accounts, mortgage loans and auditing mortgage loans.

11. In the early spring of 2018, DUDDING met a man online who said his name was Lucas Antonio Blantino or Benito (LUCAS).¹ DUDDING stated in approximately May 2018, LUCAS called her using Facebook Messenger, but she claimed she accidentally answered the call

¹ It is not known if this is the subject's real name; however, this is the name the subject used during the entire period he corresponded with DUDDING. Law enforcement believes that the same individual purporting to be LUCAS, is the individual that SUSAN GROOMS knows as Andy Mario ("MARIO").

and LUCAS began talking to her. DUDDING stated LUCAS told her he was Italian and that he had a strong accent. DUDDING admitted that she became emotionally attached to LUCAS, but never met him in person. DUDDING stated LUCAS' telephone number is 650-614-1391.

12. DUDDING advised LUCAS she was not wealthy, and he never asked her for any loans or financial gifts. LUCAS and DUDDING communicated frequently online on Facebook for a couple of months or so. LUCAS eventually told DUDDING he wanted to communicate with her on a Viber account. LUCAS also sent DUDDING numerous text messages over a 14-month period. They communicated from early spring of 2018 until June 24, 2019. Investigators later learned that DUDDING has still been communicating with LUCAS as recently as July 30, 2019.

13. LUCAS advised DUDDING he worked on an oil rig. Sometime in early 2018 or mid-summer 2018 he was moving temporarily to the United Kingdom to work on an oil rig, on a major project. He told DUDDING a major piece of equipment he owned broke down and he did not have the funds to make the repairs. However, LUCAS never asked DUDDING for any money from her personally. Instead, LUCAS told DUDDING he was going to borrow money from a financier in Africa. The investigation has revealed that DUDDING lost very little of her own personal money from financial transactions with LUCAS.

14. LUCAS then asked DUDDING to set up numerous bank accounts in her name, at different banks including People's Bank, Branch Banking & Trust ("BB&T"), SunTrust Bank, Community Trust Bank, JP Morgan Chase Bank, First State Bank, United Bank, Wes Banco, and Huntington Federal Savings Bank. DUDDING received numerous deposits from at least 23 different individuals located domestically and abroad in the bank accounts that she either opened or held on LUCAS' behalf. DUDDING informed law enforcement that she has never spoke with

or met any of the individuals who either transferred money into her bank accounts or sent her checks which she deposited into her bank accounts. DUDDING elaborated she has never communicated via email or text message with any of these individuals.

15. LUCAS would contacted DUDDING via Viber calls or text messages to tell her how much money he was going to have deposited into her account. Each time after LUCAS would have wire transfers sent to her personal bank account, LUCAS would also call her on the Viber account or text her and tell her when to send a wire transfer to Nigeria or make other disbursements.

16. After DUDDING sent numerous wire transfers to Nigeria, numerous banks, including BB&T and People's Bank closed DUDDING's accounts due to suspected fraudulent activity. The investigation revealed JP Morgan Chase Bank has frozen DUDDING's bank account due to suspected illegal activity.

17. In or around July of 2019, DUDDING informed investigators that she suspected that these accounts were involved in illicit activities.

18. Investigators analyzed DUDDING's bank account information and learned that there had been multiple financial transactions between DUDDING and SUSAN GROOMS. Specifically, GROOMS made at least four transfers into DUDDING's Chase bank account that has been frozen by bank officials. The wire transfers were as follows: \$19,000.00 and \$38,500.00 transferred on March 13, 2019; \$19,200.00 transferred on March 20, 2019; and \$19,200.00 transferred on March 27, 2019.

19. Investigators then went to interview SUSAN GROOMS who voluntarily admitted that she had sent about \$200,000 to DUDDING's bank account at the direction of Andy Mario (hereinafter, "MARIO").

20. GROOMS showed S/A Hedrick a photo of MARIO and let S/A Hedrick copy photos of Andy MARIO's photo from the subject device. Upon S/A Hedrick's examination, it appears that the photo of MARIO is the same photograph of LUCAS that DUDDING showed investigators previously. Investigators believed that the same individual is purporting to be both MARIO and LUCAS.

21. GROOMS also told S/A Hedrick that she uses her phone to communicate with MARIO on a daily basis. The investigation has not revealed any evidence that GROOMS communicated with MARIO on any other device, such as a laptop or an Ipad.

22. The affiant submits that there is probable cause to believe that the subject device is GROOMS' personal phone for the following reasons: (1) GROOMS called your affiant from the mobile number 937-424-7713; and (2) your affiant personally saw GROOMS holding an Iphone during their conversation at which time she indicated that was the user of that Iphone.

23. When investigators asked GROOMS during the voluntary interview if they could search the subject device, she refused and told your affiant that she did not want to let investigators search the subject device because there was information on her phone (the subject device) from MARIO that she did not want to share with the investigators.

24. Based on my training and experience, I believe that GROOMS' statement shows that GROOMS used the subject device to communicate with MARIO.

25. Thus, based on the affiant's training and experience as well as his personal observations, there is probable cause that the subject device — an Iphone assigned the number 937-424-7713 — is GROOMS' personal phone and the phone that she used to communicate with MARIO.

26. GROOMS further explained to investigators that she met MARIO about two years ago from an online dating website. GROOMS stated that she became friends with MARIO, and now considers MARIO more than a friend. When asked how much of her own money she had given MARIO, she estimated she had sent about \$4,000. When GROOMS first met MARIO, he was living in California. Shortly after they started to communicate online, MARIO told GROOMS he was moving to England to work on a \$1,000,000 pipeline job for a hospital. Not long afterwards, Mario allegedly went to England he told Grooms that some of his equipment had broken down and he needed money to repair the equipment or replace the equipment.

27. GROOMS has never met MARIO in person but GROOMS speaks to MARIO on the phone or via text or email, all of which are accessible on the subject device, almost on a daily basis. GROOMS stated that early on MARIO called her on the following phone numbers (650) 332-9036 and (323) 642-6641. GROOMS stated that MARIO also used the phone number 144-65-29254773. Lately, GROOMS admitted that she used the Viber App² to communicate with Mario.

28. MARIO asked GROOMS if he could have some people wire transfer money into her bank account and then have her to wire transfer the money to other people, who would then wire transfer the money to his financier so he would have the funds needed to repair or replace his equipment. GROOMS asked MARIO why he just did not have these people to wire transfer

² **Viber** uses the users phone number as their "identity" and lets them make free **Viber** phone calls to any friends who have **Viber** - using their phone number. Users can make calls and send texts via WiFi, as well as via 3G.

the money straight to his bank account in England. According to GROOMS, MARIO explained that he did not have a company bank account or a personal bank account in England. GROOMS stated she thought that was odd but, MARIO convinced her to allow people to wire transfer money into her account and that she would then transfer the money to others. MARIO always contacted GROOMS when he was having someone wire transfer money into GROOM's account.

29. GROOMS has held numerous bank accounts at least eight different banks over the past two years. When asked by investigators why she had so many accounts at different banks she admitted that many of the banks had closed her accounts because of all the wire transfers and deposits into her accounts from individuals located across the United States. GROOMS admitted that numerous bank officials (from different banks) advised her that the activity in and out of her bank accounts was very unusual. GROOMS stated that the bank officials further elaborated that they believed the wire transfers into her account were illegal proceeds and that they had seen similar schemes where money was being sent to Nigeria.

30. GROOMS stated that each time a bank closed her account she would tell MARIO. GROOMS also claimed she had informed MARIO that the bank officials at several banks told her the funds coming into her account were illegal. According to GROOMS, MARIO repeatedly told her that the bank officials were incorrect and that all of the deposits were from legitimate sources of income.

31. GROOMS admitted to investigators that she has never communicated with or met any of the people she received money from or sent wire transfers. Instead, GROOMS claimed that she was simply following instructions from MARIO.

32. GROOMS received wire transfers or checks from several individuals across the United States.

33. GROOMS has sent money via wire transfers and checks to the following persons: PATRICIA DUDDING, COLLEEN BISHOP, and Benjamin Amedu.

34. GROOMS provided the following documents and information: Fed Ex receipts wherein she sent Fed Ex packages to Benjamin Amedu in Baltimore, MD; COLLEEN BISHOP in Montana, GROOMS also provided paperwork proving that she wire transferred \$29,000 to Benjamin Amedu on or about 3/28/2019.

35. GROOMS also had deposits from STRIPE INC. totaling \$105,000 in March 2019.

36. GROOMS told investigators that she has never sent any funds to Nigeria. Investigators, however, later located in records that GROOMS provided, information suggesting that she had in fact sent money to Nigeria. Specifically, GROOMS made handwritten notes of the a bank address, located in Nigeria, and the address of a Nigerian company. PATRICIA DUDDING used the same address for a wire transfer over \$1,000,000 to an account held by Keibler Couture Ltd., at this same Nigerian bank.

37. GROOMS sent \$800.00 to "Peter Grooms" in Nigeria on January 13, 2018 via Money Gram; that same day, GROOMS sent another \$2,000.000 to "Peter Groom" in Nigeria on via Money Gram.

38. GROOMS provided a receipt which showed on January 22, 2019 she sent a 2009 Toyota Corolla to Nigeria through Prestige Shipping in New Jersey. The cost for shipping this vehicle was \$1,200. GROOMS paid for the shipping with funds from a bank account, which is believed to be part of this international wire fraud, mail fraud and money laundering scheme. Prestige Shipping provided documents about this transaction and the company records reflect this vehicle was shipped to Edward Osayi in Nigeria.

39. GROOMS purchased six iPhones for \$4,370.34 from an Apple store in Beavercreek, OH on or about January 13, 2018. GROOMS then sent the iPhones via Fed Ex to Kenneth Eboh in Benin City, Nigeria.

40. Based on my experience in conducting counterfeit and financial crimes for over twenty years, I have found that suspects often use devices such as the subject device listed in this warrant to research on the internet for items needed to commit their crime, to seek information on their crime and learn techniques to defeat discovery. Suspects may also use devices, such as the subject device, to communicate with others regarding their illegal activities. For example, the suspect may correspond with an innocent victim that has no idea the suspect plans to pay them with illegally obtained funds. The suspect may also use devices, such as the subject device to correspond with someone who is a co-conspirator. This correspondence may be in the form of telephone calls, text messages or emails. From the facts alleged above, it appears that the MARIO and GROOMS communicated almost exclusively through text messages, phones calls, or other forms of communication on her subject device. Any GPS and mapping information on the subject device may identify areas GROOMS and associates may have committed fraud or indicate a time period that she was in a certain area.

41. The subject device is currently in the possession of Susan Grooms, who resides at 814 Princeton Avenue, Fairborn, OH 45324. I seek out this warrant to search 814 Princeton Avenue for the subject device. There is probable cause to believe that the subject device will be located here, as this address is the residence of SUSAN GROOMS, who investigators believe possesses the subject device.

42. The facts alleged above establish probable cause that the evidence will be found on the subject device of the alleged violations of 18 U.S.C. § 1028 (identity theft), 18 U.S.C.

§ 1343 (wire fraud), and 18 U.S.C. §§ 1956-1957 (money laundering). I am also requesting this warrant to be certain that an examination of the subject device will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

43. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- c. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

44. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online I know that the electronic devices, such as the subject device, have capabilities that allow them to search and store information. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

45. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

46. As described above and in Attachment B, this application seeks permission to search for the subject device at 814 Princeton Avenue. Thus, the warrant applied for would also authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information in the subject device, all under Rule 41(e)(2)(B).

47. *Probable cause.* I subject that if the subject device is found at 814 Princeton Avenue, there is there is probable cause to believe that things that were once stored on the subject device may still be stored there, for at least the following reasons:

- e. Based on my knowledge, training, and experience, I know that computer or other electronic device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed

via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer or other electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer or other electronic device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- g. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer or other electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer or other electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

48. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the subject device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the subject device because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- j. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or other electronic device, or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer or other electronic device was remotely accessed, thus inculcating or exculpating the computer or other electronic device owner. Further, computer, electronic device, and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers and other electronic device typically contain information that log: user account session times and durations, activity associated with user accounts, electronic storage media that connected with the computer or other electronic device, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer, other electronic device, or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer, electronic device or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or other electronic device may both show a particular location and have geolocation information

incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer or other electronic device may provide relevant insight into the computer or other electronic device user's state of mind as it relates to the offense under investigation. For example, information within the computer or other electronic device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic device, computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- k. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- l. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- m. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how the electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- n. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

49. *Necessity of seizing or copying entire subject device or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the subject device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how the subject device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at 814 Princeton Avenue. However, taking the subject device and storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the subject device to human inspection in order to determine whether it is evidence described by the warrant.

51. As described in Attachment A, the subject device is an Apple brand device, specifically an iPhone.

52. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

53. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

54. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short

time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

55. The passcode or password that would unlock the subject device is not known to law enforcement. Thus, it will likely be necessary to press the fingers of SUSAN GROOMS, the user of the subject device, to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device via Touch ID with the use of the fingerprints of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

56. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of 814 Princeton Avenue to press their fingers against the Touch ID sensor of the locked subject device found during the search of the 814 Princeton Avenue in order to attempt to identify the device's user and unlock the subject device via Touch ID.

57. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the subject device as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

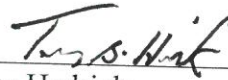
58. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at 814 Princeton Avenue, including SUSAN GROOMS, to the Touch ID sensor of the subject device for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

59. There is probable cause to believe that the subject device contains evidence of GROOMS' criminal activities specifically, because (1) GROOMS showed S/A Hedrick pictures of the man she believed to MARIO on the subject device; (2) GROOMS stated that she speaks to MARIO on from her phone daily, and (3) GROOMS refused to allow the investigators to search the subject device during their interview and stated she did not want to them to see some of her conversations with MARIO that were on the subject device.

60. Thus, I submit that this affidavit supports probable cause for a search warrant for the residence located at 814 Princeton Avenue to search for and seize the subject device, and authorization for the examination of the subject device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Terry Hedrick
Special Agent
USSS

Subscribed and sworn to before me
on August 20, 2019:



MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

1. The property to be searched is as follows:
 - a. 814 Princeton Avenue, Fairborn, OH 45324.
 - b. An Iphone Smart Phone, assigned to number 937-424-7713 (the “subject device.”) The subject device is currently located in the possession of Susan Grooms, 814 Princeton Avenue, Fairborn, OH 45324.

This warrant authorizes the forensic examination of the subject device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the subject device described in Attachment A that relate to violations of 18 U.S.C. 1028 (identity theft), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §§ 1956 - 1957 (money laundering) and involve SUSAN GROOMS, PATRICIA DUDDING, COLLEN BISHOP, Faith Campbell, Sharri Caldwell, Carolyn Gray, Benjamin Amedu, Beverly Ezernack, Ramanarce Moonilal, Robert Skiles, Betty Backer, Teresa Cobb, Lourdes Boschuk, Ram International Intimacy Fund and Andy MARIO, since on or about January 01, 2017 including:
 - a. Any record of a business locations or other addressed which would identify recent travel history of all the above including internet search, any map program, and/or GPS information found on the subject device.
 - b. Any email, text message, or voice mail message via text, found on the subject device which would identify persons to whom GROOMS exchanged United States currency during a business or personal monetary transaction of any kind.
 - c. Any photographs or identifying information of potential overseas suspects.
2. Evidence of user attribution showing who used or owned the subject device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the execution of the search of the 814 Princeton Avenue described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at 814 Princeton Avenue, including SUSAN GROOMS, to the Touch ID sensor of the subject device for the purpose of attempting to unlock the subject device via Touch ID in order to search the contents as authorized by this warrant.